Implications of The New EU Regulations Targeting Mobile Payment Fraud

May. 2019

80%

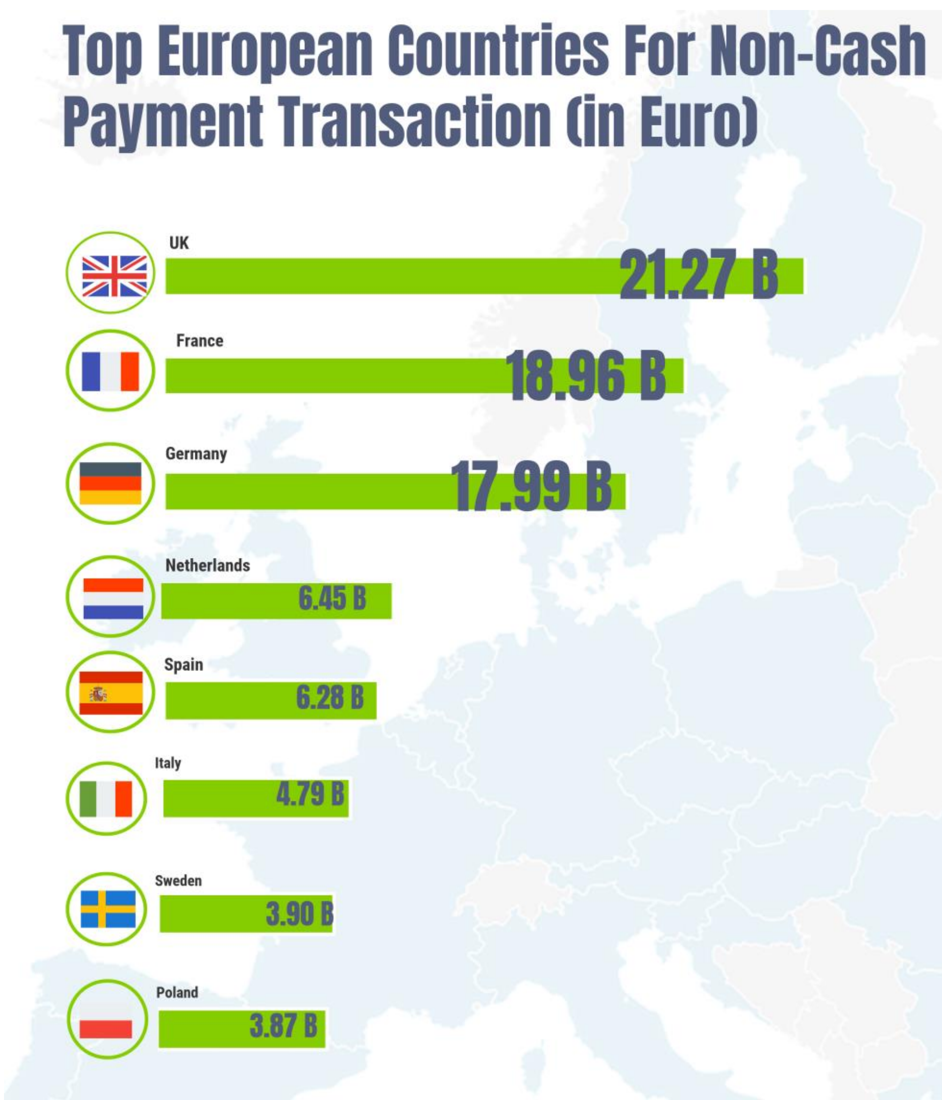
of European citizens use their mobile devices for making purchases

Pan-European survey, Visa, 2018

The EU is becoming more vigilant against fraud involving non-cash payments, including mobile transactions, online transactions, and credit cards. It recently (April 2019) passed a regulation that updates existing edicts to ensure that a strong, and technology-agnostic legal framework is in place. It also removes operational obstacles that impede investigation and prosecution and foresees actions to enhance public awareness of fraudulent techniques such as phishing or skimming.

Why Now?

In the past decade the adoption of non-cash payments has dramatically increased throughout Europe. While in 2010 10% of the EU population used non-cash payments to transact, today the numbers have increased exponentially. Most European countries have embraced digital payments, some have made it its main means of payment. Case in point is Sweden, where digital payments supersede cash payments.



75%

of the Europeans used shopping apps for their mobile commerce in the past year

Pan-European survey, Visa, 2018

While digital payments have increased, EU regulations to protect consumers and curb non-cash related fraud have not kept pace. While PSD2 was the main European security edict of the past decade, it mainly focused on financial institutions, open banking and some degree eCommerce. PSD2 reference to cryptocurrencies, digital wallets, and other digital payments was partial. The need for a comprehensive and focused regulation for digital payments was lacking.

As cashless payments have grown in during the past decade, so has fraud. Payment related fraud has reached staggering levels and with the rise of new transaction alternatives to cash such as cryptocurrencies, digital wallets and other the need for adjustment to the dated guidelines was necessary.

The EU commission realized that modernizing and upgrading the existing guidelines was required – as much of the guidelines were outdated. The new regulations impact on guidelines established out in 2001. It was obvious that the rules no longer reflect today's realities and do not sufficiently address new challenges and technological developments.

What New?

The directive aims to be technology-neutral and encompass not only traditional non-cash payments such as bank cards or cheques but also new ways of making payment such as digital wallets, mobile payments and crypto currencies.

Some of the main provisions are:

- Establishing clear definitions of online (digital payment) crime offences
- Setting guidelines regarding offences and penalties for cybercriminals and fraudsters who engage in elicit payment activities: five, four or three years of prison, depending on the offence, as the minimum penalty in cases where a judge imposes the national "maximum" custodial sentence for non-cash payment fraud;
- Assistance and support to ensure victims are sufficiently informed of their rights and citizens are advised on how to protect themselves from such frauds;
- Clarification of the scope of jurisdiction to ensure cross border fraud is tackled more effectively

The directive provides for base rules, so member states are free to go further and implement more rigorous local guidelines, including a broader definition of offences, accountability and consequences.

73%

of European payment fraud is via CNP

FSS Payment Report, 2018

Key Provisions and Directives

What does provision mean for PSPs and Merchants?

The new regulation shows resemblance to PSD2 in its early days. In its infancy, PSD2 was misunderstood and market players looked at each other in confusion to see who will adopt it first. But once the regulation became widely accepted, organizations began to scramble to embrace it.

It appears that the new regulation is ushering in a new era for non-cash payments in Europe that is likely to be a catalyst for a larger digital payment revolution.

Although early to say, the regulation may dramatically impact the payments industry. Merchants and their PSPs counterparts need to start thinking clearly about how best to comply with the new provisions. The introduction of best-in-class risk-based fraud solutions will be an important piece of the puzzle. It will be essential for PSP and large retailers who rely on digital payments as a revenue source to keep fraud and friction at a minimum while keeping regulators happy.

Although regulatory initiatives require adaptation, they also create opportunity. Organizations who embrace and integrate strong fraud guidelines as part of their processes will lead them market.

About Paygilant

Paygilant employs a CMA authentication methodology that it calls SmartRISK that makes mobile payments safer, faster and easier.

Using a disruptive technology that is designed to protect mobile payments, either executed by NFC, QR code or online, from mobile fraud, Paygilant operates in a hybrid mode on the mobile device and back-end server. Paygilant enables friction-less customer experience prior to processing the transaction, triggering immediate authentication only upon a suspicious fraudulent attempt.

Financial institutions, eCommerce and mobile wallet providers decisively stop fraud while dramatically enhancing their customers experience. What makes Paygilant a breakthrough is that it does not rely on **Behavioral Biometrics** as the sole criteria for authentication, rather incorporates additional fraud indicators including **Device Indicators** and **Transaction Analysis**. Paygilant's SmartRISK combines **Device Indicators, Behavioral Biometrics** and **Transaction Analysis** to decisively identify fraudsters from legitimate customers.